

PAT-NO: JP02003178164A
DOCUMENT-IDENTIFIER: JP 2003178164 A
TITLE: LICENSE MANAGING DEVICE, LICENSE
MANAGING METHOD AND
LICENSE MANAGING PROGRAM
PUBN-DATE: June 27, 2003

INVENTOR-INFORMATION:

NAME	COUNTRY
HATAKEYAMA, TAKAHISA	N/A
YOSHIOKA, MAKOTO	N/A
MIYAZAWA, YUJI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
FUJITSU LTD	N/A

APPL-NO: JP2002270625

APPL-DATE: April 6, 1999

INT-CL (IPC): G06F017/60, G06F012/14 , G06F015/00 ,
H04L009/08

ABSTRACT:

PROBLEM TO BE SOLVED: To provide flexible contents utilization control and accurate prevention of fraudulent utilization of contents to an information provision authority.

SOLUTION: A copyright holder system 20, a contents server 30, a license server 40 and a user system 50 are provided. An ACL setting part 23 of the copyright holder system 20 sets a plurality of partial utilization permission

conditions with respect to the contents as structurally
represented utilization
permission conditions ACL by a combination of logical sums
and logical products
on the basis of a user ID and IDs of a plurality of
physical elements including
a medium used in the user system 50, and stores them in an
access control list
43. The license server 40 encrypts the access control list
43 and a decipher
key Kc by combining the plurality of physical element IDs.

COPYRIGHT: (C)2003,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-178164

(P2003-178164A)

(43) 公開日 平成15年6月27日 (2003.6.27)

(51) IntCl ⁷	識別記号	F I	テラポート(参考)	
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2	5 B 0 1 7
	3 0 2		3 0 2 E	5 B 0 8 5
	5 1 2		5 1 2	5 J 1 0 4
12/14	3 2 0	12/14	3 2 0 A	
			3 2 0 F	

審査請求 有 請求項の数15 OL (全 25 頁) 最終頁に続く

(21) 出願番号 特願2002-270625(P2002-270625)
 (62) 分割の表示 特願平11-99482の分割
 (22) 出願日 平成11年4月6日(1999.4.6)

(71) 出願人 000005223
 富士通株式会社
 神奈川県川崎市中原区上小田中4丁目1番
 1号
 (72) 発明者 島山 卓久
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72) 発明者 吉岡 誠
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (74) 代理人 100089118
 弁理士 酒井 宏明

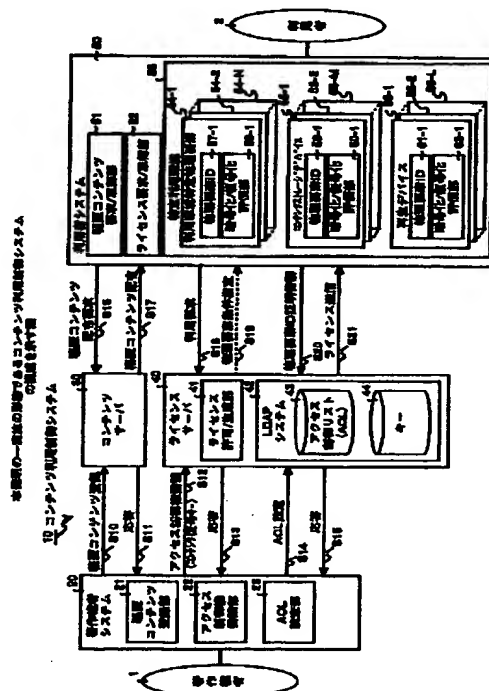
最終頁に続く

(54) 【発明の名称】 ライセンス管理装置、ライセンス管理方法およびライセンス管理プログラム

(57) 【要約】

【課題】 情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができる。

【解決手段】 著作権者システム20とコンテンツサーバ30とライセンスサーバ40と利用者システム50とを有し、著作権者システム20のACL設定部23は、利用者システム50で使用するメディアを含む複数の物理要素のIDおよび利用者IDに基づいてコンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件ACLとして設定し、アクセス制御リスト43に格納する。ライセンスサーバ40は、このアクセス制御リスト43と復号キーKcを複数の物理要素IDを組み合わせで暗号化する。



【特許請求の範囲】

【請求項1】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置であって、

前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶した物理要素経路記憶手段と、

前記物理要素経路記憶手段により記憶された物理要素の10 情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手段と、を備えたことを特徴とするライセンス管理装置。

【請求項2】 前記物理要素経路記憶手段により記憶された物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成手段は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項1に記載のライセンス管理装置。

【請求項3】 前記ライセンス生成手段は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項2に記載のライセンス管理装置。

【請求項4】 前記物理要素経路記憶手段により固有識別子が記憶された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成手段は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項2または3に記載のライセンス管理装置。

【請求項5】 前記ライセンス生成手段は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項4に記載のライセンス管理装置。

【請求項6】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理方法であって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録工程と、前記物理要素経路登録工程により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成工程と、を含んだことを特徴とするライセンス管理方法。

【請求項7】 前記物理要素経路登録工程により登録さ

れた物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成工程は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項6に記載のライセンス管理方法。

【請求項8】 前記ライセンス生成工程は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項7に記載のライセンス管理方法。

【請求項9】 前記物理要素経路記憶工程により固有識別子が記憶された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成工程は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項7または8に記載のライセンス管理方法。

【請求項10】 前記ライセンス生成工程は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項9に記載のライセンス管理方法。

【請求項11】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理プログラムであって、

前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録手順と、

前記物理要素経路登録手順により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手順と、をコンピュータで実行することを特徴とするライセンス管理プログラム。

【請求項12】 前記物理要素経路登録手順により登録された物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成手順は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項11に記載のライセンス管理プログラム。

【請求項13】 前記ライセンス生成手順は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項12に記載のライセンス管理プログラム。

【請求項14】 前記物理要素経路登録手順により固有

識別子が登録された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成手順は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項12または13に記載のライセンス管理プログラム。

【請求項15】 前記ライセンス生成手順は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項14に記載のライセンス管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化されたコンテンツを復号する復号鍵とともにコンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に回答して復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムに関する。

【0002】貨幣の役割は、その貨幣という物質としての性質によって、公平な報酬を人々に提供する。貨幣というオブジェクトは、単なる口約束の共有概念ではなく、物理的に存在し、携帯でき、さらに発行元以外による偽造が困難であることが必須要件であった。物理的に存在し、携帯できることによって、その価値の利用者どうしで公平に確認することができ、偽造の困難性によって、その公平な確認の契機を公平なる貨幣の発行元がコントロールすることができた。しかし、近年の工業技術の発展によって、今や貨幣の偽造困難性が崩壊する日が近い。貨幣に代わる新たな価値確認オブジェクトが必要になっている。そのオブジェクトはやはり、まず物理的に存在し、携帯でき、偽造困難である必要がある。さらにそのオブジェクトは発行元がアクセスコントロールできる必要がある。

【0003】このセキュリティ強化面からの要求に加え、情報流通の多様化と大容量化、高速化の側面から「超流通」の実現の要求も高まっている。この「超流通」を実現した環境は、つぎの条件を満足する。すなわち、(1) 情報利用者は、デジタル情報をほぼ無料で入手できること、(2) 情報提供者は、その情報の利用を許可する条件(課金、改変利用条件など)を指定し、利用者の合意した条件を強制することができること、(3) このサービスを利用するに当たって、必要な情報利用者の追加操作は「アクセス条件の確認」程度であること、である。

【0004】こうした超流通のアクセス制御を正確かつ、安全に実行可能なシステムは、ライセンス料などの著作権料徴収の不公平の是正にも寄与することが期待できる。現行システムでは、著作物が相当数売れないと提供者は利益を上げられないが、正確に著作権者の手に渡

るようにシステムを構築できることが望まれる。また、専門家的芸術家から、部品としての創作を提供するデザイナーに至るまで、各人のサービス料に見合う報酬が公平に分配されることが望まれる。

【0005】

【従来の技術】従来、著作物等のコンテンツに対するアクセスを分散システム環境、特に開放ネットワーク上において制御する場合、コンテンツの利用者からのアクセスが可能なサーバにコンテンツを格納し、このサーバに対するアクセスを制御することによって、コンテンツの利用を制御していた。ここで、コンテンツとは、単一の記憶装置媒体に記録可能なビット列の集合としての構造をもつデジタルコンテンツであり、文書テキスト、画像、動画、プログラムソフトウェア等を含む。

【0006】たとえば、図17は、従来のアクセス制御モデルを示す図である。図17において、コンテンツ204は、アクセス制御機能203を介してのみ、利用者205からのコンテンツ操作を可能としている。また、著作権者200は、コンテンツ204をアクセス制御機能203で保護された、たとえばサーバに登録するのみで、著作権者200以外の者、たとえばこのサーバを管理する管理者によってアクセス制御機能203に対するアクセス制御操作がなされていた。

【0007】すなわち、図18に示すようにコンテンツを保持するサーバシステム212は、管理者201によって管理運用されるサーバ運用者システム211によって管理され、サーバ運用者システム211は、サーバシステム212に対して著作権者および利用者登録を行い、またこのためのディレクトリ生成を行い、さらに、著作権者によるアクセス制御を許可することも行う。著作権者システム210は、著作権者の著作物のコンテンツをサーバシステム212に保存させ、アクセス制御条件(ACL)をサーバシステム212に対して設定する。この場合、著作権者は、サーバシステム212に対してアクセス制御の許可を得なければならない。一方、利用者システム213は、コンテンツの利用に際して、コンテンツ送信要求をサーバシステム212に対して行い、ACLを満足する場合には、サーバシステム212内に保存されていたコンテンツを取得する。

【0008】しかし、コンテンツの利用者にすべての権限が与えられ、移動やコピー(複製)によって利用者が変わると、移動あるいはコピー先のコンテンツに対しては、もとの著作権者の権限はまったく働かない。また、コンテンツオブジェクトを保存するサーバ管理者と著作権者の間では、オブジェクトに対するアクセス許諾強制のあり方も明確ではなく、たとえばサーバ管理者が著作権者に断りなく、アクセス権を変更可能なことが当然のこととされていた。

【0009】一方、近年の記憶媒体等の低価格化等によって分散システム環境が促進され、ネットワークのトラ

フィックが集中することなく、コンテンツを複数のサーバにキャッシュして分散できるようになり、コンテンツオブジェクトに対するアクセスを高速に行うことができるようになった。従って、図17に示すようなアクセス制御モデルは、利用者205によるコンテンツ操作への入り口のみに対して強固なアクセス制御機能を構築すればよいが、上述した分散システム環境下では、全方向的なアクセス制御あるいはセキュリティ保護を行う必要があった。

【0010】そこで、図19に示すようなアクセス制御モデルが考えられた。このアクセス制御モデルでは、著作権者200が従来のセキュリティ技術で保護が可能な領域である著作権者保護領域と、あらゆる外部からの攻撃を受容する開放領域と、ハード/ソフトの改ざんの保護とデジタルデータ複製防止処理が施される秘匿保護領域とに分離される。秘匿保護領域は、全方向的なアクセス制御機能221によって保護し、このアクセス制御機能221内にコンテンツ222が保存される。

【0011】このコンテンツに対して、著作権者200は、コンテンツ222の登録とともに、アクセス制御機能221に対するアクセス制御操作も可能としている。利用者205は、開放領域から、アクセス制御機能221を介してコンテンツ222を取得することになる。なお、領域間保護インターフェース220は、著作権者保護領域と開放領域との間の保護を行うインターフェースである。

【0012】この図19に示す分散システム環境下におけるアクセス制御モデルの具体化は、米国特許5339403号公報に記載されており、また、特開平9-134311号公報、米国特許5392351号公報、米国特許555304号公報、および米国特許5796824号公報には、利用者の機器をチェックしてコンテンツの不正利用を防止する技術が記載されている。以下、これらの公報を参照して従来のコンテンツ利用制御システムについて説明する。

【0013】図20は、従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。図20において、復号保護領域と再生保護領域とは、図18に示す秘匿保護領域に相当し、復号保護領域は、ハード/ソフトの改ざんの保護と出力データの複製防止保護の領域であり、再生保護領域は、デジタル復号データの複製防止の領域である。利用環境特定物理要素(PCSUE)235-1~235-Nは、コンテンツの利用環境を特定する物理要素であり、具体的には、CPU、周辺装置、リムーバブルな記憶媒体、ICカード等である。

【0014】復号保護領域では、PCSUE235-1~235-Nに対応する物理要素IDの証明書236-1~236-Nをもとに、著作権者200によって暗号化されたコンテンツ233の複製であって開放領域のサーバに存在するコンテンツ234を復号し、再生保護領

域を介して、この複合されたコンテンツが利用者に利用される。従って、コンテンツは、物理要素IDに対応したキーで暗号化され(コンテンツ233)、このコンテンツ233に対応するコンテンツ234を復号するためには、各物理要素IDまたはそれに対応した秘密のキーが必要となる。

【0015】ここで、コンテンツ配布モデルには、暗号化されたコンテンツを復号するために用いられるライセンスを、暗号化されたコンテンツと同時に配布するライセンス同時モデルと、暗号化されたコンテンツをサーバのキャッシュに保存し、ライセンスとは別のタイミングで取得するコンテンツキャッシュ可能型モデルとがある。図21は、このコンテンツキャッシュ可能型モデルを示す図である。

【0016】図21において、まず著作権者200は、著作権者保護領域で、コンテンツを生成し、このコンテンツを暗号化し、その後、複製して開放領域のサーバ等にキャッシュされる。一方、PCSUE235-1~235-Nの物理要素IDを暗号化した証明書241-1~241-Nは、暗号化された状態で著作権者保護領域に出力され、PCSUE235-1~235-Nに対応する利用者物理オブジェクトクラスから秘密キーKpを取り出し、この秘密キーKpと証明書241-1~241-Nとから物理要素ID243-1~243-Nを復号し、この物理要素ID243-1~243-Nによってコンテンツ復号キーKcを暗号化し、秘密保護領域に出力する。

【0017】秘密保護領域では、暗号化されたコンテンツ復号キーKcを物理要素ID242-1~242-Nで復号し、コンテンツ復号キーKcを得る。このコンテンツ復号キーKcを用いて開放領域から取得される、暗号化されたコンテンツ234を復号し、コンテンツ244として利用者205に利用させる。

【0018】図22は、図21に示すコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示すブロック図である。図22において、著作権者システム250は、著作権者保護領域に存在し、コンテンツサーバ251は、開放領域に存在し、ライセンスサーバ252および利用者システム253は、秘匿保護領域に存在する。著作権者システム250は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ251に保存しておく。

【0019】また、コンテンツ復号キーKcをライセンスサーバ252に送信して、アクセス制御権の委譲をライセンスサーバ252に対して行う。さらに、アクセス制御リスト(ACL)設定を行う。利用者システム253は、コンテンツを利用することを示す利用要求をライセンスサーバ252に送信し、このとき、物理要素IDの証明群が添付されていない場合には、ライセンスサー

バ252の物理要素条件指定によって物理要素IDの証明群を取得し、ライセンスサーバ252に送出する。

【0020】ライセンスサーバ252は、図21に示したように、利用者の物理オブジェクトクラスの秘密キーKpを取得して物理要素ID証明群を復号し、復号した物理要素IDによって暗号化されたコンテンツ復号キーKcがライセンスLとして利用者システム253に送出される。これによって、利用者システム253の物理要素IDが一致すれば、復号が行われ、この復号されたコンテンツ復号キーKcを用いて秘匿コンテンツを復号することが出来る。

【0021】なお、秘密コンテンツはコンテンツサーバ251に保存されているので、利用者システム253は、別途コンテンツサーバ251に秘密コンテンツ配布要求を行って、コンテンツサーバ251から秘密コンテンツの配布を受ける必要がある。

【0022】一方、図23は、コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成ブロック図を示している。図23では、コンテンツサーバ251が存在せず、ライセンス送信と同時に利用者システム253に送付されることになる。図22に示すように、コンテンツサーバ251を介して秘密コンテンツを取得する場合、秘密コンテンツは予め時間的に利用者システム253に近いサーバまで運ばれているので、利用者システム253は、コンテンツが必要な時に利用要求をすればよい。

【0023】また、コンテンツ同時配布型モデルと比較してコンテンツの流通経路の適切な選択が可能となり、利用者にとっては、コンテンツ取得に際して応答時間の短縮が期待できる。また、コンテンツキャッシュ可能型モデルでは、コンテンツを、ライセンスの提供とは別に、ROM媒体ベース、放送、Proxyサーバによるキャッシュ等によって、予め配布しておくことが可能であり、利点が多い。

【0024】

【発明が解決しようとする課題】しかしながら、上述した従来のコンテンツ利用制御システムでは、利用者システムに固有の物理要素IDに一致する装置であれば、基本的に秘匿コンテンツを復号でき、このコンテンツを利用することができるが、この物理要素IDのみによってライセンス（利用許可条件）を生成しているので、たとえば、著作権者の意思で決定されるコンテンツの読み出し回数を制限する条件を付加したり、時間制限を設けたり、課金条件を設定したりすることができず、柔軟なコンテンツ利用制御ができないという問題点があった。

【0025】また、利用環境特定物理要素は、常に単純な構成となつてとは限らず、複雑な構成をもった機器である場合には、その機器のうちの特定の機器あるいは部品が不正である場合もあり、このような場合に、単に大きな構成の機器である利用環境特定物理要素によって

利用許可条件を生成しても、不正を見逃してしまうこととなりセキュリティが低下するという問題点があった。

【0026】この発明は上記に鑑みてなされたもので、著作権者等の情報作成者に許諾された者を含む情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができるライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムを提供することを目的とする。

10 【0027】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置であって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶した物理要素経路記憶手段と、前記物理要素経路記憶手段により記憶された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手段と、を備えたことを特徴とする。

【0028】この発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶し、記憶した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成することとしたので、コンテンツの不正利用を精度高く防止することができる。

【0029】また、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理方法であって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録工程と、前記物理要素経路登録工程により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成工程と、を含んだことを特徴とする。

40 【0030】また、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に応答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理プログラムであって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録手順と、前記物理要素経路登録手順により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手順と、をコンピュータで実行すること

を特徴とする。

【0031】かかる発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録し、登録した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成することとしたので、コンテンツの不正利用を精度高く防止することができる。

【0032】

【発明の実施の形態】以下に添付図面を参照して、本発明にかかるライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムの好適な実施の形態を説明する。

【0033】図1は、本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。図1に示すコンテンツ利用制御システム10は、著作権者1が作成した著作物のコンテンツを利用者2が利用する場合に、この利用を制御するシステムである。図1において、このコンテンツ利用制御システム10は、大きく、著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、および利用者システム50を有する。

【0034】著作権者システム20は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ30に登録する(S10)処理を行う秘匿コンテンツ登録部21、暗号化したコンテンツ(秘匿コンテンツ)を復号するのに必要なコンテンツ復号キーをライセンスサーバ40に送出することによって、アクセス制御権をライセンスサーバに委譲する(S12)処理を行うアクセス制御権委譲部22、および利用許可条件(ACL)をライセンスサーバ40に設定する(S14)ACL設定部23を有し、著作物のコンテンツに関する利用制御を管理する。

【0035】コンテンツサーバ30は、著作権者システム20から送られた秘匿コンテンツを登録し、利用者システム50からの秘匿コンテンツ配布要求があった(S16)場合に、この登録され、保存されている秘匿コンテンツを暗号化された状態で利用者システム50に送出する(S17)。

【0036】ライセンスサーバ40は、ライセンス許可/生成部41とLDAPシステム42とを有する。ライセンス許可/生成部41は、利用者システム50からコンテンツの利用要求があった(S18)場合、この利用要求に付加された物理要素ID証明書とこれに対応する復号キーをLDAPシステム42から検索し、物理要素IDを復号し、利用要求されたコンテンツに対応するコンテンツ復号キーを検索し、この検索したコンテンツ復号キーを物理要素IDで暗号化したライセンスを送信する(S21)。

【0037】このライセンスは、物理環境特定要素条件であり、物理要素の構造に対応させ、論理和と論理積を用いて構造化した組み合わせの形態となっている。ま

た、この実施の形態では、従来から用いられていた物理環境特定要素条件のみならず、利用者の利用状況を条件とした会計条件も併せてACLとして暗号化される。このライセンスの暗号化と復号化については後述する。なお、利用要求(S18)に物理要素ID証明書が付加されていない場合、LDAPシステム42内にも存在しない場合には、物理要素条件指定(S19)を利用者システム50に送付して、利用者システム50が生成した物理要素ID証明書群を返す(S20)。

10 【0038】一方、著作権者システム20からアクセス制御権委譲によるコンテンツ復号キーが送られてきた(S12)場合は、このコンテンツ復号キーを後述するLDAPシステム42内のキー44のデータベースに秘匿コンテンツに対応させて登録する。また、著作権者システム20からACL設定が送られてきた(S14)には、このACLを秘匿コンテンツに対応させて、LDAPシステム42内のアクセス制御リスト(ACL)に格納する。

20 【0039】利用者システム50は、秘匿コンテンツの配布要求(S16)と配布された秘匿コンテンツの取得を行う秘匿コンテンツ要求/取得部51と、ライセンスの要求、すなわち利用要求(S18)とライセンスの取得(S21)の処理を行うライセンス要求/取得部52と、利用者システムの特定利用環境(SUE)53とを有する。特定利用環境53とは、特定のコンテンツ利用環境をいい、CPU、周辺装置、リムーバブルな記憶媒体、ICカード、コンテンツ利用状況などの総合的情報をいう。

30 【0040】特定利用環境には、CPU等の利用環境特定物理要素(PCSUE)54-1~54-Nと、コンテンツを格納するコンテンツストレージデバイス55-1~55-Mと、プレーヤやビューワ等の再生デバイス56-1~56-Lとを有する。各PCSUE54-1~54-N、各コンテンツストレージデバイス55-1~55-M、および各再生デバイス56-1~56-Lは、それぞれの物理要素ID57-1~57-N、59-1~59-M、61-1~61-Lを有するとともに、暗号化/復号化/評価部58-1~58-N、60-1~60-M、62-1~62-Lを有する。

40 【0041】暗号化/復号化/評価部58-1~58-N、60-1~60-M、62-1~62-Lは、各物理要素を暗号化する場合には、自物理要素の物理要素IDで暗号化して出力し、各物理要素の復号化を行う場合には、自物理要素の物理要素IDで復号化を行い、さらに復号結果を評価する処理を行う。すなわち、各物理要素IDの処理に関しては各物理要素毎に行い、物理要素間のインターフェース上であっても、情報が漏れないようにしている。

50 【0042】つぎに上述した著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、利用者シ

システムの動作処理を主としてフローチャートを参照して説明する。まず、図2のフローチャートを参照して、著作権者システム20の内部処理手順について説明する。

【0043】図2において、著作権者システム20は、まず操作イベントが発生したか否かを判断する(ステップS100)。操作イベントが発生していない場合(ステップS100、なし)には、操作イベントが発生するまでこの処理を繰り返し、操作イベントが発生した(ステップS100、あり)には、操作イベントの操作内容が秘匿コンテンツ登録か、ACL登録か、アクセス制御権委譲かを判断する(ステップS101)。

【0044】操作内容が秘匿コンテンツ登録である場合(ステップ101、秘匿コンテンツ登録)には、秘匿コンテンツ登録部21は、コンテンツの暗号化を行い(ステップS110)、コンテンツサーバリストから所望のコンテンツサーバ30を指定し(ステップS111)、この指定したコンテンツサーバ30に対して秘匿コンテンツ登録要求を行う(ステップS112)。その後、コンテンツサーバ30からの応答を得て、その応答がOKであるかエラーであるかを判断する(ステップS113)。

【0045】コンテンツサーバ30からの応答がOKの場合にはそのまま、エラーである場合には、エラー処理を行った(ステップS114)後、さらに、つぎのコンテンツサーバが指定されたか否かを判断する(ステップS115)。つぎのコンテンツサーバが指定された場合(ステップS115、あり)には、ステップS112に移行して上述した処理を繰り返し、つぎのコンテンツサーバが指定されていない場合(ステップS115、なし)には、ステップS100に移行して上述した処理を繰り返す。

【0046】操作内容がACL設定である場合(ステップ101、ACL設定)、ACL設定部23は、さらに、指定されたコンテンツ復号キーを登録するか否かを判断し(ステップS120)、コンテンツ復号キーの登録をしない場合(ステップS120、なし)には、エラー処理を行って(ステップS124)、ステップS100に移行し、上述した処理を繰り返す。一方、コンテンツ復号キーの登録がある場合(ステップS120、あり)には、ACL設定要求をライセンスサーバ40に送信し(ステップS122)、ライセンスサーバ40からACL登録結果を受信し(ステップS123)、その後ステップS100に移行して上述した処理を繰り返す。

【0047】また、操作内容がアクセス制御権委譲である場合(ステップS101、アクセス制御権委譲)には、暗号化したコンテンツ復号キーをライセンスサーバ40に送信し(ステップS130)、暗号化コンテンツ復号キーの登録結果を受信し(ステップS131)、ステップS100に移行し、上述した処理を繰り返す。

【0048】つぎに、ここで、ACL設定部23によ

て設定されるACLについて説明する。図3は、アクセス条件の一例を示す図であり、アクセス条件は、会計条件と物理環境特定要素(PCSUE)条件との2種類がある。図3に示すように、本発明の特徴の一つである会計条件としては、まず、maxCount(操作可能回数最大値)があり、これに対応するコンテンツの利用状況はcount(操作済回数)である。操作済回数という可変値に対して操作可能回数最大値という制限を設けてアクセスを制御、すなわち限定と認可を行おうとするものである。

【0049】つぎのmaxLength(読み出し最大長さ)の会計条件値に対応するコンテンツの利用状況は、totalLen(読み出し済長さ+被請求読み出し長さ)であり、コンテンツの読み出し最大長さによってアクセスの制御をしようとするものである。つぎのmaxTimeLen(実行可能最大時間)の会計条件値に対応するコンテンツの利用状況は、totalTime(実行済時間長)であり、コンテンツの実行可能最大時間によってアクセスの制御をしようとするものである。つぎのmaxDebt(借入可能金額(課金条件))の会計条件値に対応するコンテンツの利用状況は、debt(残金)であり、残金のマイナス値は借入金額となり、課金条件によってアクセスの制御をしようとするものである。

【0050】また、物理環境特定要素条件としては、まず計算機本体があり、これに対応する物理要素IDのクラスは、PSNであり、プロセッサのシリアル番号である。ここで、クラスとはデータベース上のオブジェクトクラスである。つぎの周辺デバイスに対応する物理要素IDのクラスは、DSNであり、デバイスの種類とシリアル番号を示す。つぎのメディアに対応する物理要素IDのクラスは、MSNであり、メディアの種類とシリアル番号を示す。つぎのICカードに対応する物理要素IDは、certificatesであり、ICカードが発行する証明書を示す。

【0051】つぎの人体部位は、たとえば指紋や網膜(アイリス)情報であり、これに対応する物理要素IDのクラスは、bodyPartsであり、人体部位の認証情報である。つぎの許可する時間帯に対応する物理要素IDのクラスは、timePeriodであり、ローカルクロックやグローバルなGPS時刻である。つぎのネットワークドメインは、ネットワーク上のエリアを示し、これに対応する物理要素IDのクラスは、MACAddressであり、MACアドレスを示す。つぎの地理的位置は、利用国などを示し、これに対応する物理要素IDのクラスは、locationであり、GPSあるいはPHSが検出する位置を示す。つぎの人の記憶に対応する物理要素IDのクラスは、user-ID WithPwdであり、ユーザIDとパスワードを示す。最後のグループに対応する物理要素IDのクラスは、groupであり、物理要素IDの集合を示す。

【0052】このようなアクセス条件は、ANDとOR

との論理的な組み合わせをもったセット、すなわちACLとして設定される。アクセス条件には、上述したように会計条件と物理環境特定要素条件とがあるが、これらは任意に組み合わせ可能である。たとえば、一つのACLとしては、つぎのようなものが設定される。すなわち、

```
udac_acl
```

```
read:((grop=sysrapOR group=soft4soft) AND
45661244<MSN<45661412) OR count<1;
```

```
modify:user=yujiOR user=hataOR
```

```
IC_card=1afd234fe4def458c3bac78497bbda6f;
```

```
print:group=sysrap;
```

のようなACLを設定することができる。

【0053】この設定されたACLによれば、「read」は閲覧条件を示し、グループが「sysrap」あるいは「soft4soft」であり、かつ、メディアシリアル番号MSNが45661244を越え45661412未満であるか、あるいは操作済回数が1未満すなわち、一度もコンテンツを利用したことがないことが閲覧のための条件となる。さらに、「modify」は更新条件を示し、ユーザ名が「yuji」あるいは「hata」であるか、あるいは「IC_card」の番号が「1afd234fe4def458c3bac78497bbda6f」であることがコンテンツ更新のための条件となる。

【0054】また、「print」は印刷出力条件を示し、グループが「sysrap」に限り、コンテンツを印刷することができる。このようなACLは、著作権者システム20から著作権者1が任意に設定することができる。このACL設定は、GUIを用いることによって操作性が向上する。なお、ACLのタイプは、操作名とともに設定するようにしてもよい。たとえば、操作名1に対してはアクセス条件(1)なる条件を選択でき、操作名2に対してはアクセス条件(2)なる条件を選択できるようにしてもよい。これにより、さらに操作性が向上する。

【0055】つぎに、図4に示すフローチャートを参照して、コンテンツサーバ30の内部処理手順について説明する。図4において、まずコンテンツサーバ30は、ネットワークイベントが入力されたか、入力された場合に秘匿コンテンツ登録要求か、秘匿コンテンツ配布要求かを判断する(ステップS200)。ネットワークイベントが入力されない場合(ステップS200、なし)には、ステップ200における判断処理を繰り返す。

【0056】ネットワークイベントが秘匿コンテンツ登録要求である場合(ステップS200、秘匿コンテンツ登録要求)には、この登録要求された秘匿コンテンツを内部登録し(ステップS210)、デフォルトのACLを設定する(ステップS211)。そして、著作権者システム20に、この秘匿コンテンツ登録要求に対する応答を行って(ステップS212)、ステップS200に移行し、上述した処理を繰り返す。

【0057】一方、ネットワークイベントが秘匿コンテ

ンツ配布要求である場合(ステップS200、秘匿コンテンツ配布要求)には、この配布要求された秘匿コンテンツを利用者システム50に対して配布し(ステップS220)、その後、この秘匿コンテンツ配布要求に対する応答を利用者システム50に対して行い(ステップS221)、ステップS200に移行して上述した処理を繰り返す。これにより、コンテンツサーバ30を介して秘匿コンテンツを秘密状態で著作権者システム20から利用者システム50に配布することができる。この場合、トラフィックが分散され、高速転送が可能であるとともに、予め利用者システム50の近傍のコンテンツサーバまで秘匿コンテンツを保持することが可能であるので、配布処理を高速に処理することができる。

【0058】つぎに、図5に示すフローチャートを参照して、ライセンスサーバ40の内部処理手順について説明する。図5において、まず、ライセンスサーバ40は、コンテンツ利用要求のネットワークイベントが入力されたか否かを判断する(ステップS300)。ネットワークイベントが入力されない場合(ステップS300、なし)には、このステップS300の判断処理を繰り返す。

【0059】ネットワークイベントがコンテンツ利用要求である場合(ステップS300、コンテンツ利用要求)には、指定されたコンテンツのACLをLDAPシステム42から検索し(ステップS301)、さらに、この検索したACLから関連するアクセス条件を抽出し、新たなACLを生成する(ステップS302)。その後抽出した物理環境特定条件に対応する対応物理要素ID証明書があるか否かを判断し(ステップS303)、対応物理要素ID証明書がある場合(ステップS303、対応物理要素ID証明書あり)にはそのまま、対応物理要素ID証明書が無い場合(ステップS303、対応物理要素ID証明書無し)には、コンテンツの利用要求者に対して、すなわち利用者システム50に対して証明書を要求した(ステップS304)後、さらに、つぎの物理環境特定条件があるか否かを判断する(ステップS305)。

【0060】つぎの物理環境特定条件がある場合(ステップS305、あり)には、ステップS303に移行して対応物理要素ID証明書を確実に備える準備をし、つぎの物理環境特定条件がない場合(ステップS305、なし)には、コンテンツの利用要求者、すなわち利用者システム50から物理要素ID証明書群を受信する(ステップS306)。

【0061】その後、ライセンス許可/生成部41は、指定されたコンテンツ復号キーを検索し(ステップS307)、ACL内のアクセス条件を、強制可能な物理要素の証明書に並べ直す(ステップS308)。さらに、ACL内のすべてのAND/OR式を認証優先順に括弧でくくる処理を行う(ステップS309)。その後ライ

センス許可/生成部41は、この括弧でくくられたAND/OR式をもとに、ライセンスを生成するライセンス生成処理を行う(ステップS310)。そして、生成されたライセンスを利用者システム50に送信し(ステップS311)、ステップS300に移行して上述した処理を繰り返す。

【0062】ここで、生成されたライセンスと秘匿コンテンツとの関係について図6を参照して説明する。図6は、ライセンスサーバ40から利用者システム50に送信されるライセンスとコンテンツサーバ30を介して著作権者システム20から利用者システム50に送信される秘匿コンテンツとの関係を示している。

【0063】図6において、ライセンスサーバ40のACL43内には、それぞれ各秘匿コンテンツ71~75と対応づけられたシステムACL43-1~43-5が格納されている。このシステムACLをもとにその後、たとえば秘匿コンテンツ71~73に対応するシステムACLから秘匿コンテンツ71~73に対するライセンス84~86が生成され、利用者システムに送信される。このライセンス84~86は、対応する物理要素IDで暗号化されており、外部に情報が漏れることはない。利用者システム50は、ライセンス84~86からクライアントACL81~83を復号し、これらに対応する秘匿コンテンツ71'~73'を復号し、それぞれコンテンツを得ることができる。

【0064】この場合、秘匿コンテンツも暗号化されているので、セキュリティは十分である。このようにして、ACLと秘匿コンテンツとはその秘匿状態を維持しながら、それぞれ転送ルートが異なるものの、対応づけられている。なお、コンテンツサーバ30を含む転送経路を介して送られる秘匿コンテンツの状態は、仮想格納領域70として表現している。

【0065】ここで、さらにライセンスサーバ40内のLDAPシステム42について図7を参照して説明する。図7において、LDAPシステム42は、複数のLDAPサーバを有し、そのクライアントサーバとしてライセンスサーバ40が位置づけられ、ライセンスサーバ40の管理のもとに各LDAPサーバが機能することになる。LDAPサーバとは、ディレクトリサービスの標準であるX.500に含まれるDAPの軽量版のプロトコルを用いたディレクトリサーバである。LDAPサーバ内には複数のクラスに分けられ、たとえば個人情報91、システムクラス92、メディアクラス93、XMLで記述されたXML情報のクラスを有する。

【0066】そして、たとえば個人情報91のクラスにおいて、「own system」が検索されると、このシステムをシステムクラス92から「system name」によって検索し、さらにシステムクラス92内の現メディア「current media」は、メディアクラスの中からメディアクラス93を検索し、さらに、このメディアクラス93内の

コンテンツから、このコンテンツに対応したXML情報94を検索することができる。このXML情報94の中には、コンテンツに関する情報が格納されている。

【0067】ところで、利用者システム50の特定利用環境は、図8に示すレイヤを持った論理構造を有している。図8では、特定利用環境100が、アプリケーション層110とOSカーネル層111とデバイス層112との3層で構成され、各層間は、点線で示すサービスインターフェースで接続される。アプリケーション層110は、コンテンツ再生・実行アプリケーション101を有し、内部には、秘密コンテンツ復号保護ライブラリ102をプログラムモジュールとして有する。

【0068】秘密コンテンツ復号保護ライブラリ102は、ストレージドライバ103、ファイルシステム105、複数の利用環境特定物理要素ドライバ106~108、再生デバイスドライバを動作させる。ストレージドライバ103は、コンテンツストレージデバイスを駆動させ、利用環境特定物理要素ドライバ106~108はそれぞれ利用環境特定物理要素109~111を駆動させ、再生デバイスドライバ112は再生デバイス113を駆動させる。なお、一つの物理装置であっても、たとえばMO装置のようにコンテンツストレージデバイス104と利用環境特定要素109の二つの役割を担ってもよい。

【0069】図9は、利用環境特定物理要素(PCSUE)のOSカーネル層111とデバイス層112との対応関係を示している。図9に示すように、PCSUEどうしは、包含関係を持つことがある。もちろん、デバイス層112における他のデバイスも同様である。たとえば、PCSUE131の下位にはPCSUE133、134が位置づけられ、PCSUE134の下位にはPCSUE135、136が位置づけられる。このような包含関係を有するPCSUEどうしでは、物理要素ID等の情報をデータ交換することができる。

【0070】たとえば、DVD装置等のメディア再生装置のPCSUEは、DVD等のメディアのPCSUEを包含しており、コンテンツデータやメディアID情報を両者間で交換する。たとえば、PCSUE134とPCSUE135との間の情報交換である。そして、最上位のPCSUEのみがPCSUEドライバとのデータ交換を行う。たとえば、PCSUEドライバ120とPCSUE131との関係である。従って、同じデバイス層であっても、包含関係を有し、階層的な関係を有する場合がある。

【0071】ライセンスは、上述したように、特定環境に対する許諾情報であり、ライセンスを要求したクライアント環境、すなわち利用者システムの環境に固有の情報のみを含むものであり、ACLとコンテンツ復号キーKcとからなるアクセス情報を物理要素ID(PCSUE-ID)によって暗号化されたものである。

【0072】ここで、多重化されたライセンスの一例を示すと、つぎのようになる。すなわち、

【数1】

$$\{ \{ \{ \{ \{ \langle \text{アクセス情報} \rangle \mid K_5 \mid K_4 \mid K_3 \mid K_2 \mid K_1 \} \} \} \} \}$$

である。ここで、 $K_1 \sim K_5$ は、それぞれPCSUE-IDである。このライセンスは、アクセス情報は $K_1 \sim K_5$ を用いてAND条件によって結合されている。物理要素のセキュリティ強度が高い順に各PCSUE-IDを用いて多重的に暗号化するとよい。この復号化は、この逆

10 に外側のPCSUE-IDから順次復号されることになる。
【0073】また、物理要素のセキュリティ強度がほぼ同一の場合には、各PCSUE-IDを排他的論理和演算によってその結果の暗号キーによって復号できるようにしてもよい。たとえば、

【数2】

$$\{ \langle \text{アクセス情報} \rangle \mid (K_5 \oplus K_4 \oplus K_3 \oplus K_2 \oplus K_1) \}$$

のようにするとよい。これらの暗号化の多重化によ

20 て、一部の製品、すなわち一部の物理要素への攻撃成功によるコンテンツ復号キー K_c 盗難の危険性が分散されるという、リスク分散の効果をもたらすことになる。
【0074】また、複数のPCSUE-IDをOR演算子で結合する場合、すなわち、

【数3】

$$\{ \langle \text{アクセス情報} \rangle \mid K_5 + \{ \langle \text{アクセス情報} \rangle \mid K_4 + \{ \langle \text{アクセス情報} \rangle \mid K_3 + \{ \langle \text{アクセス情報} \rangle \mid K_2 + \{ \langle \text{アクセス情報} \rangle \mid K_1 \} \} \} \} \}$$

のような場合には、それぞれのPCSUE-IDで暗号化されたサブライセンス、たとえば、 $\{ \langle \text{アクセス情報} \rangle \mid K_1$ を生成し、すべてのサブライセンスを単純にOR演算して結合した値をライセンスとしてもよい。この場合、上述した暗号化の多重化を各サブライセンスにも適用し、AND、XOR、OR演算を入れ子にして組み合わせたライセンスとして生成してもよい。これによ

ても、リスク分散の効果は得られる。
【0075】つぎに、このようなライセンスの生成処理手順について図10に示すフローチャートを参照して説

40 明する。この図10に示すフローチャートは、図5のステップS310に示すライセンス生成処理手順のサブルーチンである。図5において、まず、上述したACLから1ワード読み出す(ステップS400)。その後読み出したワードが「(」であるか否かを判断する(ステップS410)。

【0076】読み出したワードが「(」である場合(ステップS410、「(」)には、ACLの読み出し現在位置を括弧内ACLの始点として記憶する(ステップS411)。その後、変数NBを「0」に設定し(ステッ

50 プS412)、さらにACLから1ワード読み出す(ステップS413)。その後、読み出したワードが「(」であるか否かを判断し(ステップS414)、「(」である場合には、変数NBに「1」を加算した(ステップS415)後、ステップS413に移行して再び、つぎの1ワードを読み出す。

【0077】一方、読み出しワードが「(」でない場合(ステップS414、その他)には、さらにこの読み出したワードが「)」であるか否かを判断する(ステップS416)。この読み出したワードが「)」でない場合、すなわちその他である場合には、ステップS413に移行し、さらにACLから1ワードを読み出す。一方、この読み出したワードが「)」である場合には、NBが「0」であるか否かを判断する(ステップS417)。NBが「0」でない場合(ステップS417、NO)には、NBの値から「1」減算し、ステップS413に移行し、さらにACLから1ワード読み出す。

【0078】NBが「0」のとき(ステップS417、YES)には、ACLの現在位置の一つ手前を括弧内ACLの終点として記憶する(ステップS419)。その後、この括弧内ACLのライセンス生成処理を行い(ステップS420)、その再帰呼び出しによる戻り値をアクセス条件ACに追加する処理を行って(ステップS421)、ステップS400に移行する。これによって括弧内のACLが生成される。

【0079】一方、読み出したワードが「(」でない場合(ステップS410、その他)には、さらに、この読み出したワードが物理要素条件または会計条件であるか否かを判断する(ステップS410)。物理条件または会計条件である場合には、この条件をアクセス条件ACに設定し(ステップS431)、この条件を強制可能な物理要素の秘密キー K_p として設定し(ステップS432)、ステップS400に移行し、さらにACLから1ワード読み出す。

【0080】読み出したワードが物理条件または会計条件でない場合(ステップS410、その他)には、さらに、この読み出したワードが「OR」であるか否かを判断する(ステップS430)。読み出したワードが「OR」である場合には、この読み出したワードから後のACLのライセンス生成処理を行う(ステップS441)。その後、さらに生成したライセンスの中にACが含まれるか否かを判断し(ステップS442)、ACが含まれる場合(ステップS442、YES)には、ステップS441によるライセンス生成処理の戻り値を用いて「{AC, hash} K_p , 戻り値」となるライセンスに設定し(ステップS443)、この生成したライセンスを返す(ステップS454)。一方、ライセンスの中にACが含まれていない場合(ステップS442、NO)には、ステップS441によるライセンス生成処理の戻り値を用いて「{ K_c , AC, hash} K_p , 戻り値」と

なるライセンスに設定し(ステップS445)、この生成したライセンスを返す(ステップS454)。

【0081】一方、読み出したワードが「OR」でない場合(ステップS430、その他)には、さらに、この読み出したワードが「AND」であるか否かを判断する(ステップS440)。読み出したワードが「AND」である場合には、この読み出したワードから後のACLのライセンス生成処理を行い(ステップS452)、このライセンス生成処理の戻り値を用いて「{戻り値, AC, hash} Kp」となるライセンスを返す(ステップS454)。

【0082】さらに、この読み出したワードが「AND」でない場合(ステップS440、その他)には、「{Kc, AC, hash} Kp」となるライセンスを返す(ステップS454)。これにより、ACLからライセンスが生成される。

【0083】つぎに、図11に示すフローチャートを参照して、利用者システム50の内部処理手順について説明する。図11において、まず利用者システム50は、コンテンツの利用要求があったか否かを判断する(ステップS500)。コンテンツの利用要求がない場合(ステップS500、なし)には、この判断処理を繰り返し、コンテンツの利用要求があった場合(ステップS500、あり)には、コンテンツの利用要求を送信する(ステップS501)。その後、物理要素の証明書の要求がライセンスサーバ40からあったか否かを判断し(ステップS502)、物理要素の証明書の要求がない場合(ステップS502、なし)には、ステップS508に移行する。

【0084】一方、物理要素の証明書の要求があった場合(ステップS502、あり)には、物理要素ID証明書を読み出し(ステップS503)、読み出し失敗したか否かを判断する(ステップS504)。読み出しに失敗した場合(ステップS504、YES)には、エラー通知をライセンスサーバに送信して(ステップS505)、ステップS500に移行する。一方、読み出しに失敗しない場合(ステップS504、NO)には、つぎの物理要素があるか否かを判断し(ステップS506)、つぎの物理要素がある場合(ステップS506、あり)には、ステップS503に移行して、つぎの物理要素ID証明書の読み出しを行って上述した処理を繰り返す。

【0085】一方、つぎの物理要素がない場合(ステップS506、なし)には、物理要素ID証明書群をライセンスサーバ40に送信し(ステップS507)、さらに受信内容がエラーかライセンスかを判断する(ステップS508)。受信内容がエラーである場合(ステップS508、エラー)には、ステップS500に移行して上述した処理を繰り返し、受信内容がライセンスである場合(ステップS508、ライセンス)には、さらに、

ライセンスを物理要素(PCSUE)1に渡し(ステップS509)、ステップS500に移行して上述した処理を繰り返す。これにより、利用者システム50は、ライセンスサーバ40からライセンスを取得することができる。

【0086】ここで、PCSUE1とは、(N-1)個のPCSUEの最初のPCSUEを示し、一般的にPCSUE*i*で示し、*i*は、1~(N-1)の整数である。そこで、各PCSUE*i*がライセンスを渡された時の内部処理手順について図12のフローチャートを参照して説明する。

【0087】図12において、まずPCSUE*i*は、受信したライセンスをKpiで復号する(ステップ600)。その後、この復号したアクセス条件AC*i*を評価し(ステップS601)、アクセス条件AC*i*の評価結果が可か不可かを判断する(ステップS602)。アクセス条件AC*i*の評価結果が不可の場合(ステップS602、不可)には、エラー処理を行って(ステップS604)、本処理を終了する。一方、アクセス条件AC*i*の評価結果が可である場合(ステップS602、可)には、この復号したライセンスをPCSUE(*i*+1)に送信し、復号を続行させ、本PCSUE*i*の内部処理を終了する。

【0088】つぎに、PCSUE(*i*+1)は、PCSUE(N)に相当し、ここでは、たとえば、再生デバイスの物理要素が内部処理を行う。この内部処理手順について図13に示すフローチャートを参照して説明する。図13において、まず、受信したライセンスをKpnで復号する(ステップS700)。その後、この復号したアクセス条件AC(N)を評価し(ステップS701)、この評価結果が可であるか、不可であるかを判断する(ステップS702)。評価結果が不可である場合(ステップS702、不可)には、エラー処理を行って(ステップS703)、本処理を終了して、結果的に秘匿コンテンツを復号することができないことになる。

【0089】一方、アクセス条件AC(N)に対する評価結果が可である場合(ステップS702、可)には、この復号したKcで秘匿コンテンツを復号し(ステップS704)、復号したコンテンツを再生デバイスが再生し(ステップS705)、本処理を終了する。

【0090】ここで、具体的なライセンスの復号処理を図14を参照して説明する。図14において、ライセンスサーバ40で生成されたライセンスは、アクセス制御リストACLとコンテンツ復号キーとを再生デバイス144の物理要素IDであるキーKpを用いて暗号化し、さらに、ストレージデバイスのデバイスシリアル番号であるDSN141とメディア142のメディアシリアル番号であるMSN143の排他的論理和の値をキーとして暗号化されたものである。

【0091】まず、ストレージデバイス140は、メデ

ィア142に書き込み不可のMSNを読み込み、この値とストレージデバイス140自身のDSNとの排他的論理和の演算を行い、この演算結果によってライセンスを復号すると、ライセンスは、{ACL, Kc} Kpとなる。この一部復号されたライセンスは、再生デバイス144に送られ、再生デバイス144は、再生デバイス144自身が有する物理要素IDであるキーKpを用いてライセンスを復号し、アクセス条件リストACLとコンテンツ復号キーKcとを取得し、アクセス条件ACLが示すアクセス条件を満足する場合に、コンテンツ復号キーKcによって復号を行うことができ、復号されたコンテンツは、再生デバイス144によって再生されることになる。

【0092】上述したライセンス要求とライセンス取得によるコンテンツ復号処理を図15に示すデータフローを参照してさらに説明する。図15において、利用者システム50内における復号保護領域では、まずコンテンツを利用するためライセンス要求処理152を物理要素ID証明書を送付してライセンスサーバ40に送出する。この際、物理要素ID証明書は、利用環境特定物理要素証明書取得処理153によって利用環境特定物理要素ID50から取得され、ライセンス要求処理152によって渡される。

【0093】一方、ライセンスサーバ40からライセンスが送信されるとライセンス取得処理156は、このライセンスを取得し、アクセス許可処理155は、ライセンス所得処理156からライセンスを取得するとともに、利用環境特定物理要素ID認証処理154が利用環境特定物理要素証明書取得処理153を介して物理要素IDを取得し、さらに会計処理157から利用状況を取得し、これらを用いて復号キーを取り出す。

【0094】そして、コンテンツ復号処理159は、コンテンツ復号キーを用いて秘匿コンテンツ158を復号し、平文のコンテンツを出力する。なお、会計処理157は、利用状況監視物理要素151に通知し、利用環境監視物理要素151によって現在の利用状況が利用に応じて自動的にデクリメントされる。

【0095】ところで、図16は、図8に示した特定利用環境の各エンティティに各処理手続きを実装した場合の保護強度への影響を示す図である。この結果から、利用環境特定物理要素所有証明書の生成は、デバイス層に実装し、会計情報保護は、ICカードによるデバイス層に実装することが好ましいことがわかる。このように、各処理手続きを実装するレイヤによっても保護強度が異なるので、レイヤ配置も考慮して図15に示す各処理機能を実装する必要がある。

【0096】なお、上述した実施の形態では、いわゆるコンテンツキャッシュ可能型モデルを基準とした構成として説明したが、これに限らず、コンテンツ同時配布型モデルを基準とした構成にも適用できるのは明らかであ

る。この場合、コンテンツサーバ30がライセンスサーバ40内に内部配置された構成として取り扱えばよい。

【0097】さらに、上述した実施の形態では、暗号化、復号化に関して、キーを用いることが前提となっているが、この場合において、秘密鍵暗号方式を用いても、公開鍵暗号方式を用いても、いずれでも実施可能であり、適応されるシステムに応じてそれぞれ適切な方式を適用すればよい。

【0098】また、上述した実施の形態に示す物理要素には、利用者システム50に固定の装置のみではなく、この利用者システム50を利用する際に用いられるメディア、すなわちCD-ROM、DVD、MO、ICカードやフロッピーディスク等の可搬型の記録媒体を含むものである。この可搬型の記録媒体が用いられる利用者システムにおいては、この利用者システムに固定の物理要素に加えて、この用いられる可搬型の記録媒体も物理要素に含まれて、コンテンツの利用制御がなされることになる。なお、利用者システム50に固定のメディア、例えば固定のハードディスク装置や固定のROM等が上述した物理要素に含まれるのは言うまでもない。

【0099】

【発明の効果】以上説明したように、本発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶し、記憶した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成するよう構成したので、コンテンツの不正利用を精度高く防止することができるという効果を奏する。

【0100】また、本発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録し、登録した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成するよう構成したので、コンテンツの不正利用を精度高く防止することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。

【図2】図1に示した著作権者システム20の内部処理手順を示すフローチャートである。

【図3】会計条件と物理環境特定要素条件との一例を示す図である。

【図4】図1に示したコンテンツサーバ30の内部処理手順を示すフローチャートである。

【図5】図1に示したライセンスサーバ40の内部処理手順を示すフローチャートである。

【図6】ライセンスサーバ40から送られるライセンスと著作権者システム10あるいはコンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図である。

【図7】図1に示したLDAPシステム42の構成を示

す図である。

【図8】特定利用環境のレイヤ論理構造を示す図である。

【図9】包含関係をもった物理要素の一例を示す図である。

【図10】ライセンス生成処理手順を示す詳細フローチャートである。

【図11】図1に示した利用者システム50の内部処理手順を示すフローチャートである。

【図12】利用関係特定物理要素によるライセンス復号 10 処理手順を示すフローチャートである。

【図13】再生デバイスの物理要素によるライセンス復号処理手順を示すフローチャートである。

【図14】ライセンスの復号過程の一例を示す図である。

【図15】ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図である。

【図16】特定利用環境の各エンティティに各処理手続きを実装した場合における保護強度への影響を示す図である。

【図17】従来におけるアクセス制御モデルを示す図である。

【図18】従来におけるアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図である。

【図19】改良したアクセス制御モデルを示す図である。

【図20】従来におけるコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。

【図21】コンテンツキャッシュ可能型モデルを示す図 30 部

である。

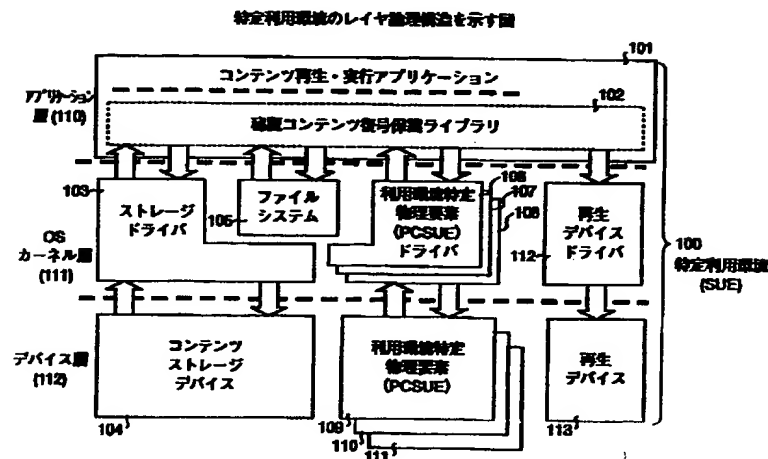
【図22】図21に示したコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示す図である。

【図23】コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図である。

【符号の説明】

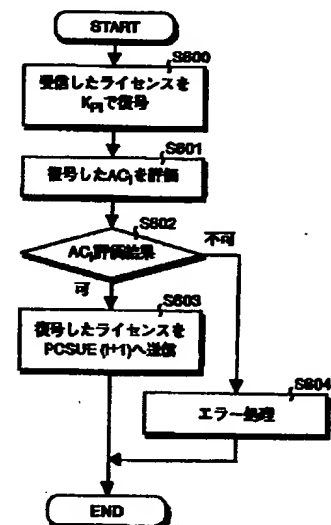
- 1 著作権者
- 2 利用者
- 10 コンテンツ利用制御システム
- 20 著作権者システム
- 21 秘密コンテンツ登録部
- 22 アクセス制御権委託部
- 23 ACL設定部
- 30 コンテンツサーバ
- 40 ライセンスサーバ
- 41 ライセンス許可/生成部
- 42 LDAPシステム
- 43 アクセス制御リスト(ACL)
- 44 キー
- 50 利用者システム
- 51 秘匿コンテンツ要求/取得部
- 52 ライセンス要求/取得部
- 53 特定利用環境
- 54-1~54-N 利用環境特定物理要素
- 55-1~55-M コンテンツストレージデバイス
- 56-1~56-L 再生デバイス
- 57-1、59-1、61-1 物理要素ID
- 58-1、60-1、62-1 暗号化/復号化/評価

【図8】

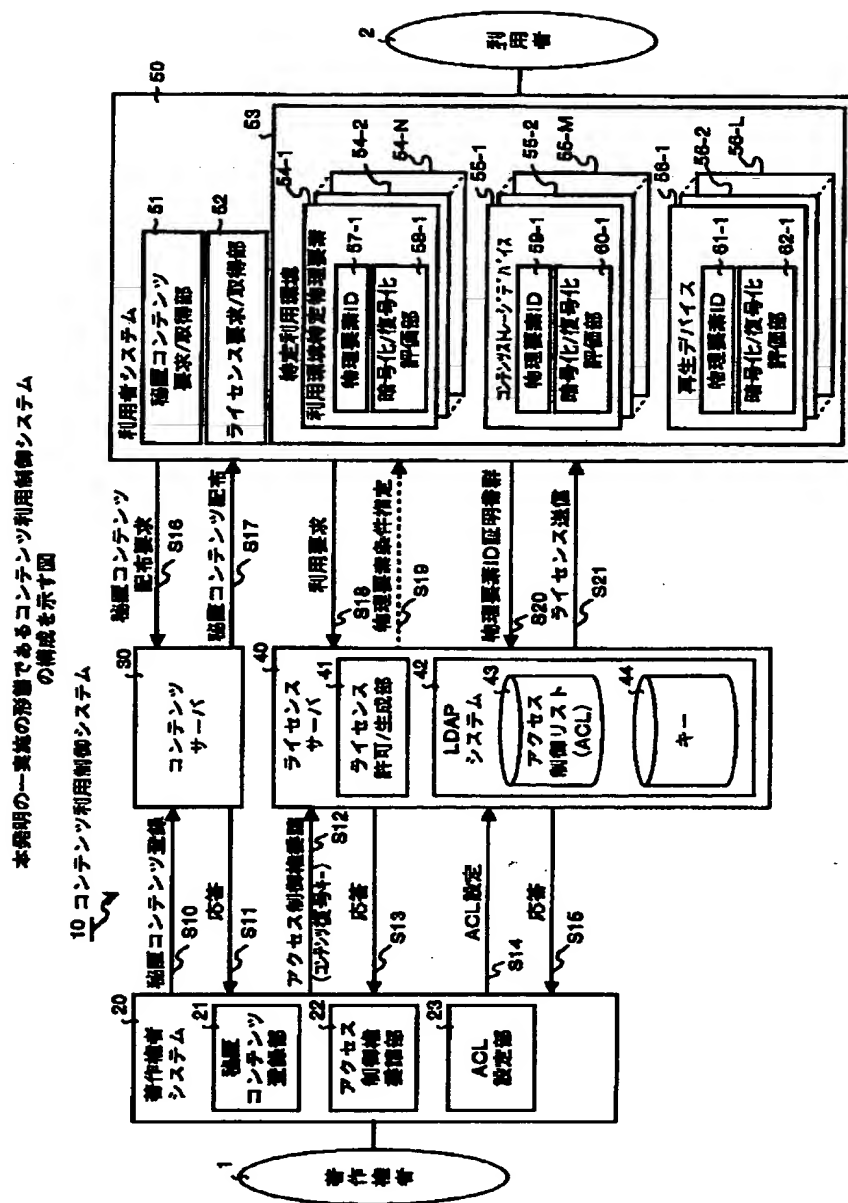


【図12】

利用関係特定物理要素によるライセンス復号処理手順を示すフローチャート

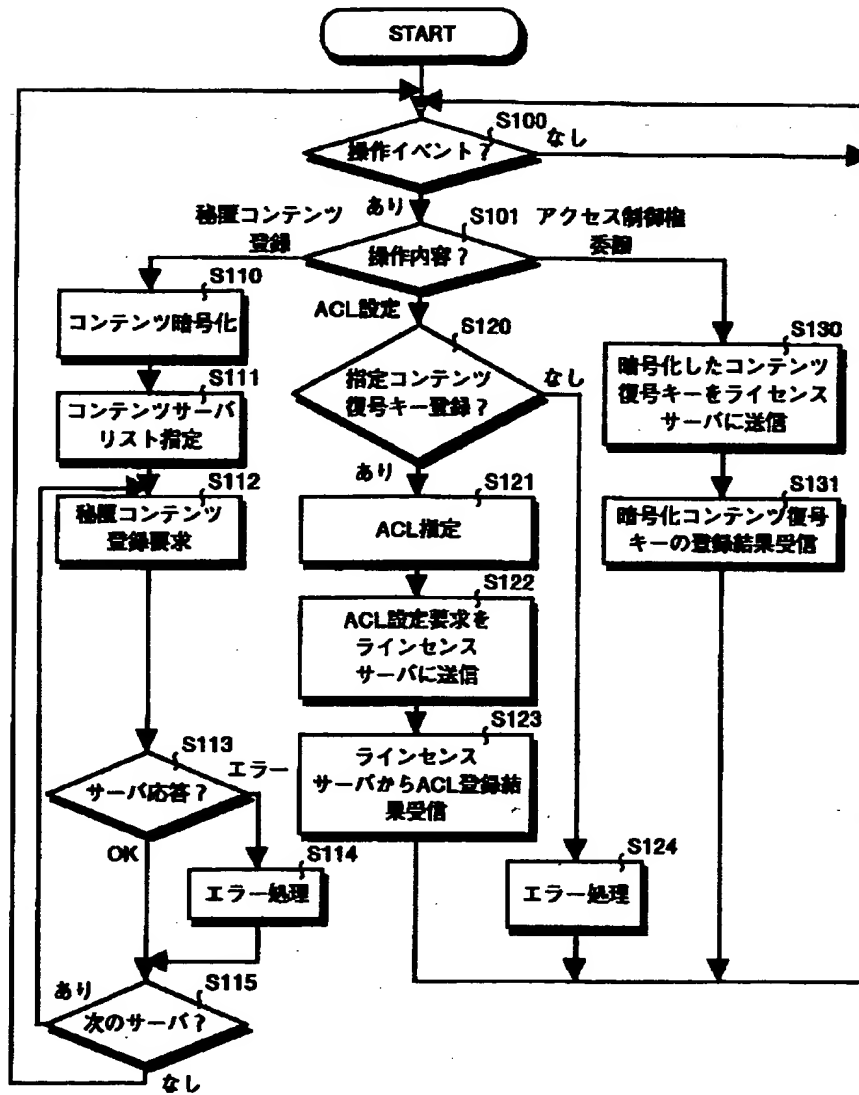


【図1】



【図2】

図1に示した著作権システム20の内部処理手順を示すフローチャート



【図3】

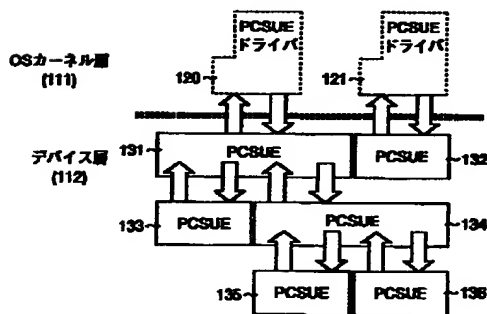
会計条件と物理環境特定要素条件との一例を示す図

会計条件値 (Account Condition Value)	利用状況 (Usage State)
max Count : 操作可能回数最大値	count : 操作済回数
max Length : 読み出し最大長さ	totalLen : 読み出し済長さ + 被要求読み出し長さ
max TimeLen : 実行可能最大時間	totalTime : 実行済時間長
max Debt : 借入可能金額 (課金条件)	debt : 残金 (マイナスは借入金額)

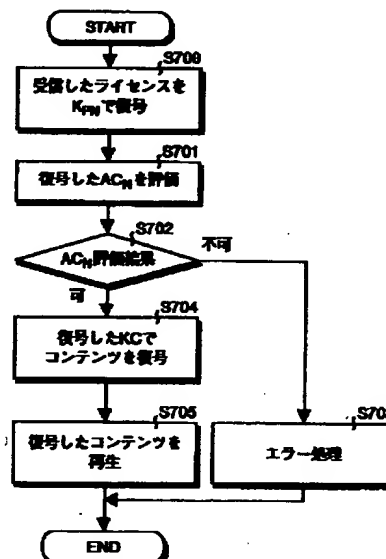
物理環境特定要素 (PCSUE) 条件	物理要素IDクラス (PCSUE-IDClass)
(1) 計算機本体	PSN (プロセッサシリアル番号)
(2) 周辺デバイス	DSN : デバイスの種別、シリアル番号
(3) メディア	MSN : メディアの種別、シリアル番号
(4) ICカード	certificates : ICカードが発行する証明書
(5) 人体部位 (指紋、網膜…)	body Parts : 人体部位 (指紋、網膜…) 認証情報
(6) 許可する時間帯	time Period : 時刻 (ローカルクロック、GPSなど)
(7) ネットワークドメイン	MACAddress : MACアドレス
(8) 地理的位置 (利用国など)	location : GPS/PHS検出位置
(9) 人の記憶	user-ID WithPwd : ユーザIDとパスワード
(10) グループ	group : 物理要素IDの集合

【図9】

包含関係をもった物理要素の一例を示す図

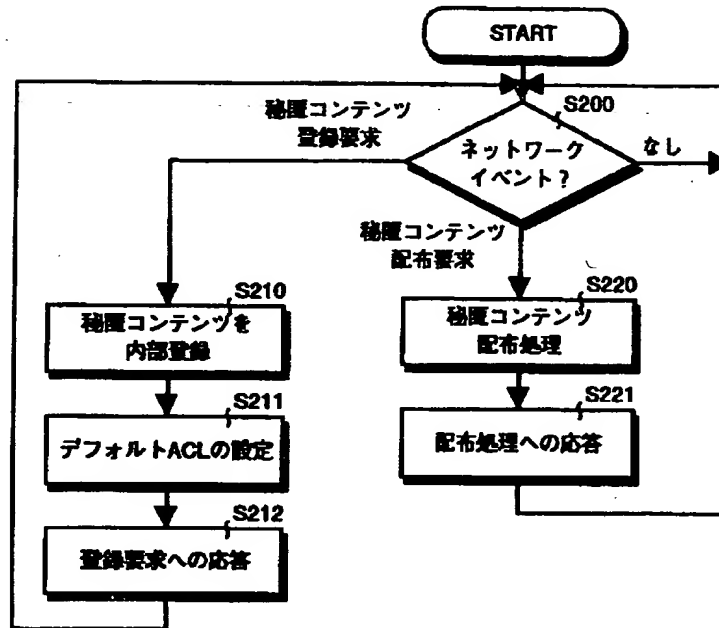


【図13】

再生デバイスの物理要素によるライセンス
番号処理手順を示すフローチャート

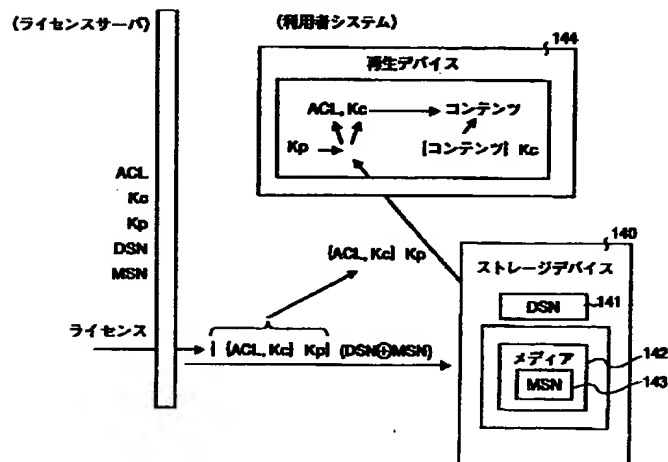
【図4】

図1に示したコンテンツサーバ30の内部処理手順を示すフローチャート



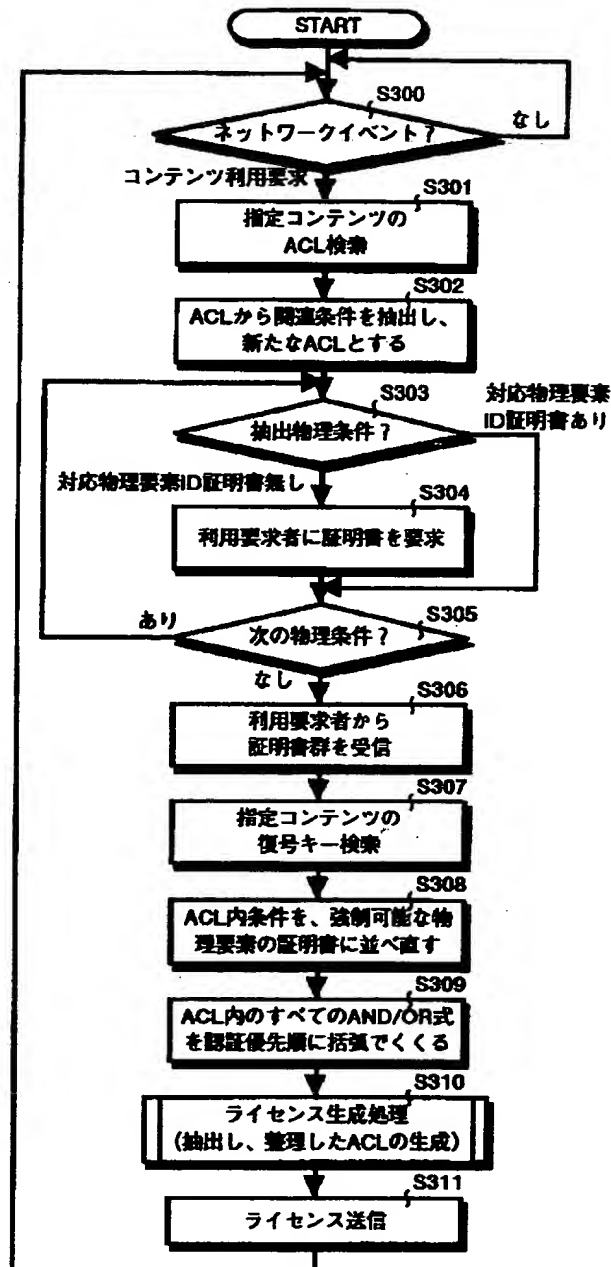
【図14】

ライセンスの番号割当の一例を示す図



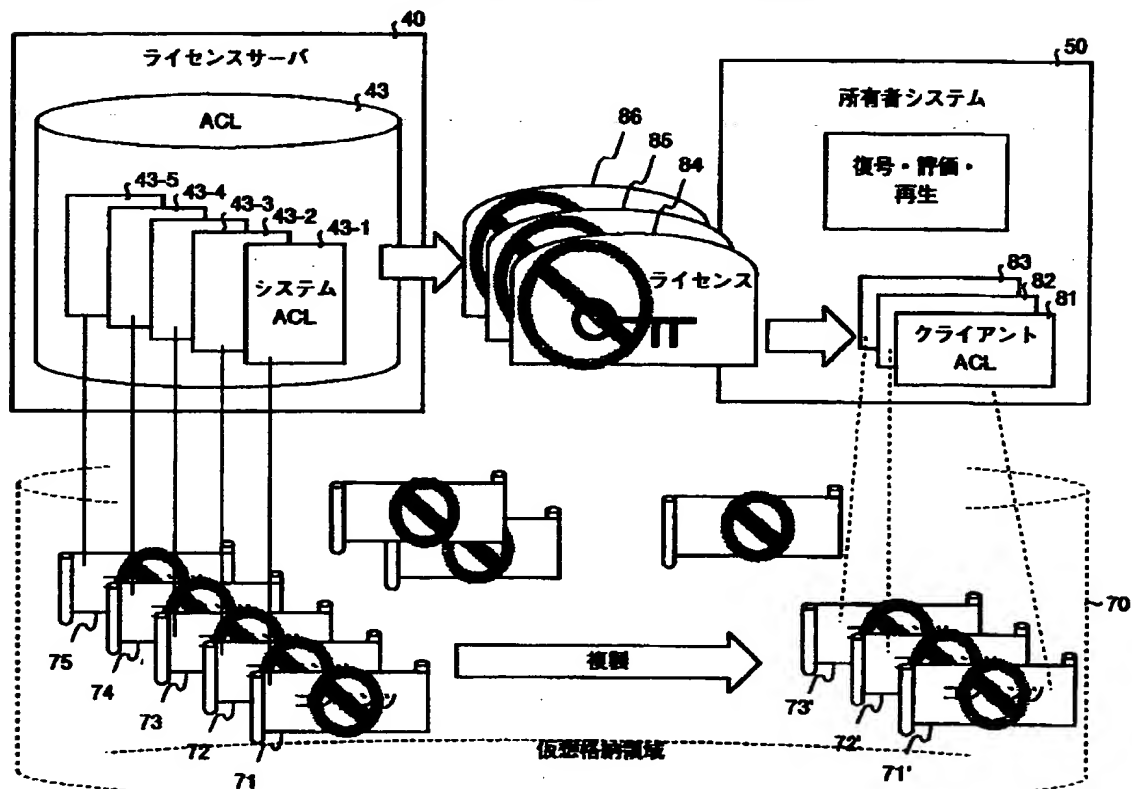
【図5】

図1に示したライセンスサーバ40の内部処理手順を示すフローチャート



【図6】

ライセンスサーバ40から送られるライセンスと著作権者システム10あるいは
コンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図



【図16】

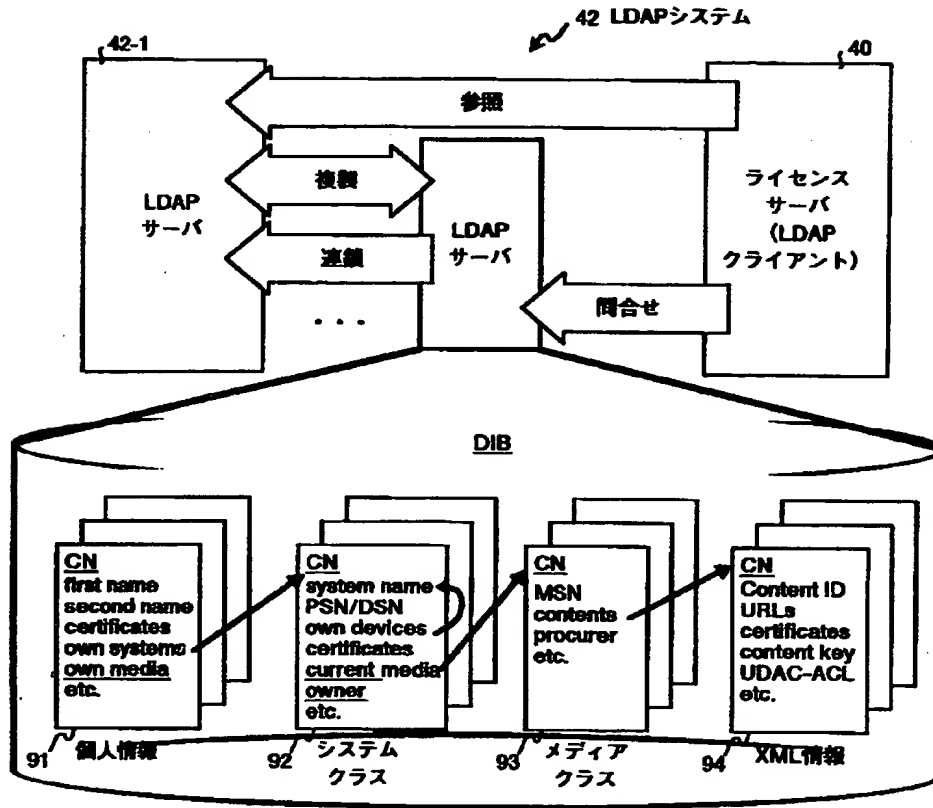
特定利用環境の各エンティティに各処理手続きを
実施した場合における秘匿強度への影響を示す図

	アプリケーション層	デバイスドライバ層	デバイス層
利用環境特定処理要素 所有権明細書生成	—	○	●
利用環境特定処理要素 の検証	○	—	—
アクセス制御リスト 検索	○	—	○
会計情報保護	△	—	○ (ICカード)
条件付アクセス許可	○	—	○
復号	○	—	○

—: 実装の意義が少ない △: 危険 ○: 専門家には保護が弱い ●: 保護が強い

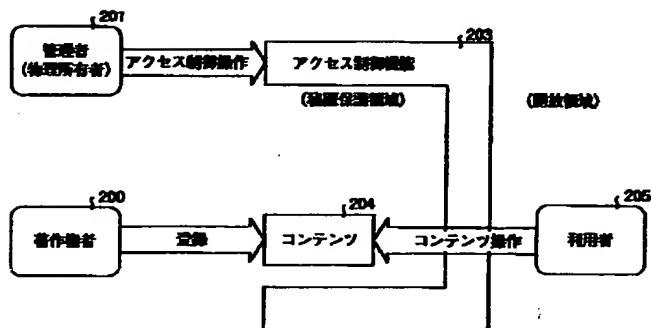
【図7】

図1に示したLDAPシステム42の構成を示す図



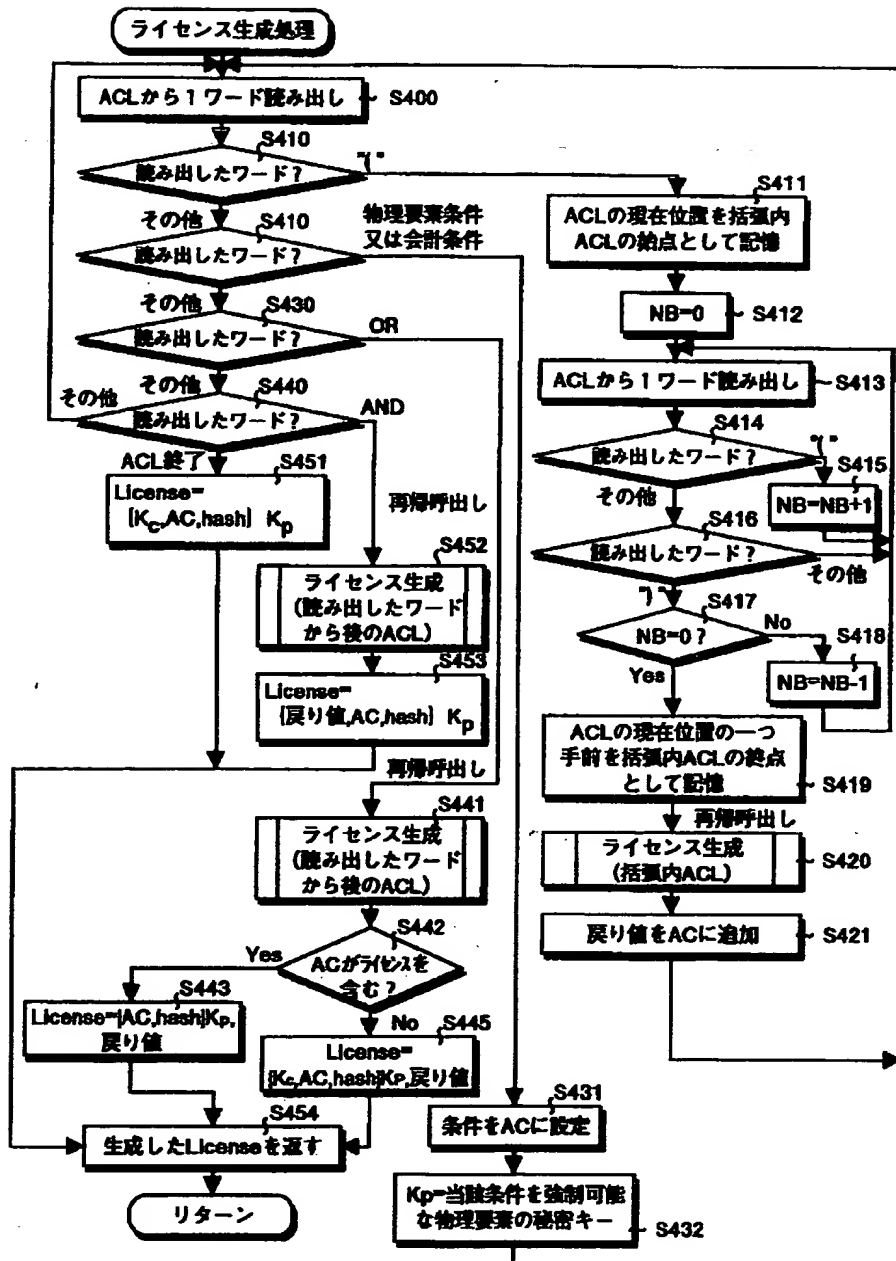
【図17】

従来のアクセス制御モデルを示す図



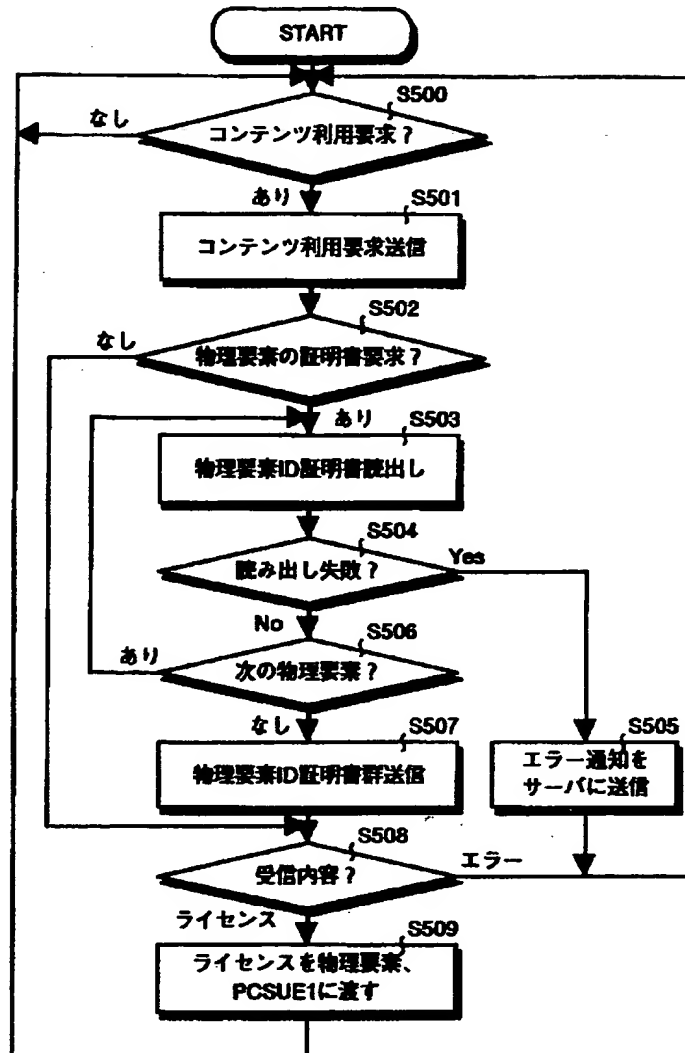
【図10】

ライセンス生成処理手順を示す詳細フローチャート



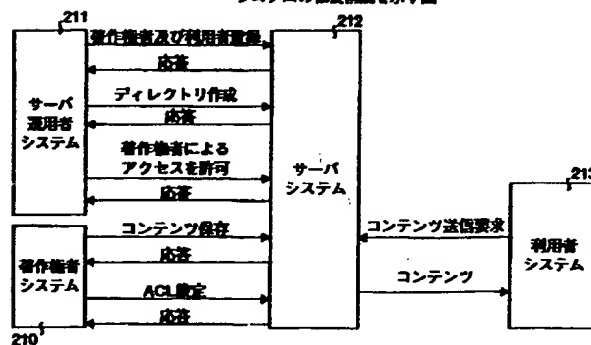
【図11】

図1に示した利用者システム50の内部処理手順を示すフローチャート



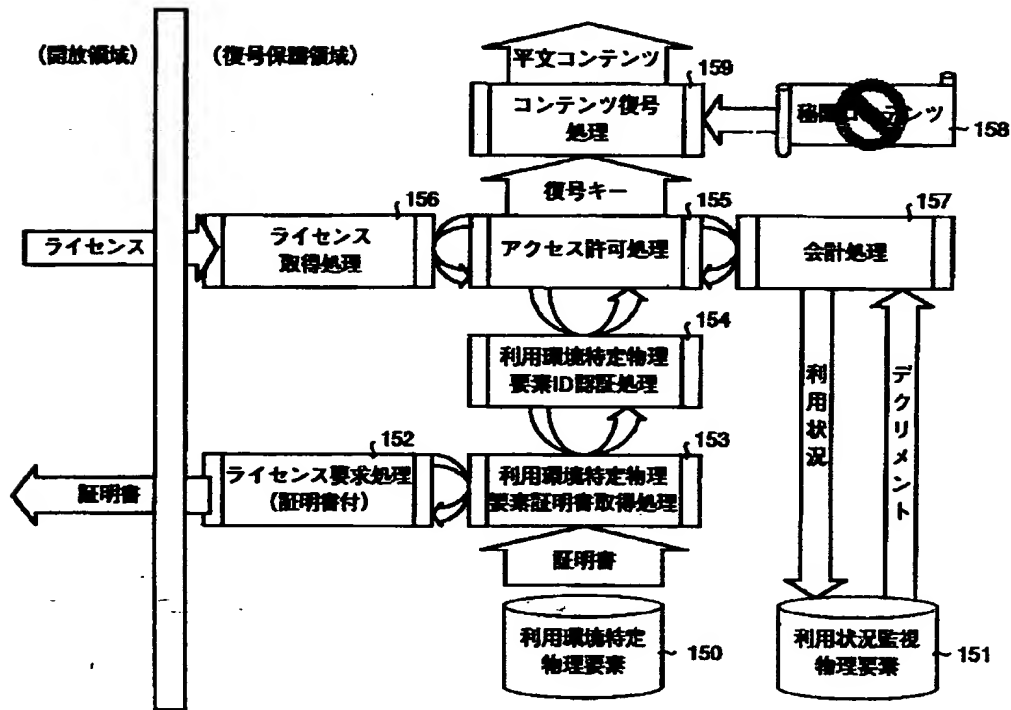
【図18】

従来のアクセス制御モデルに対応したコンテンツ利用制御システムの構成を示す図



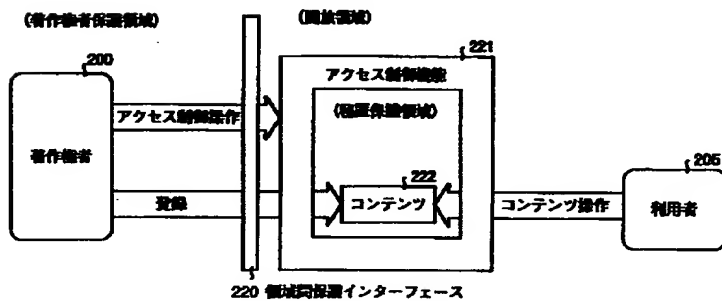
【図15】

ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図

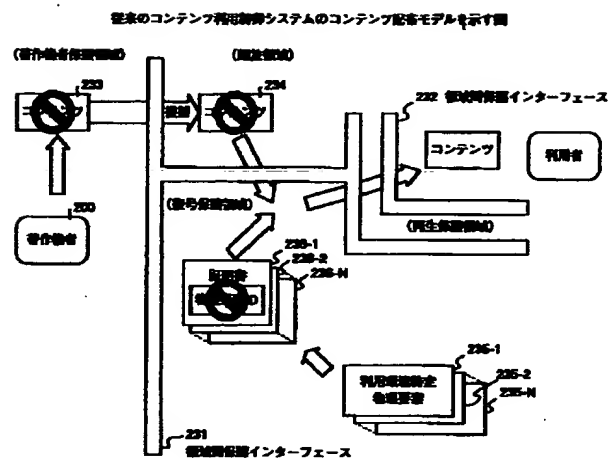


【図19】

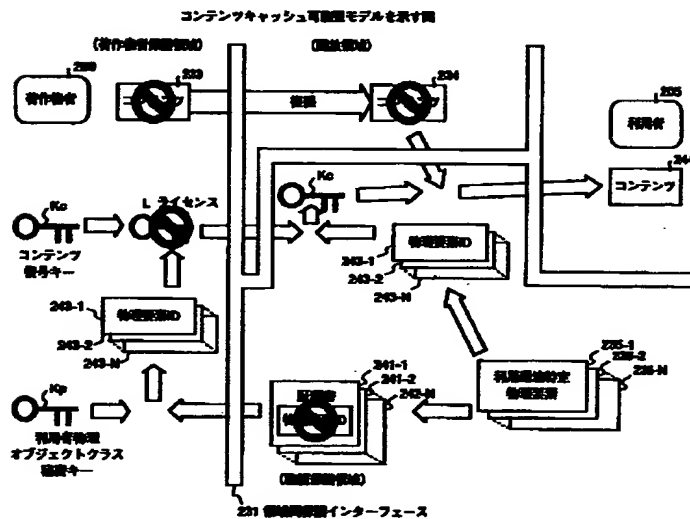
改良したアクセス制御モデルを示す図



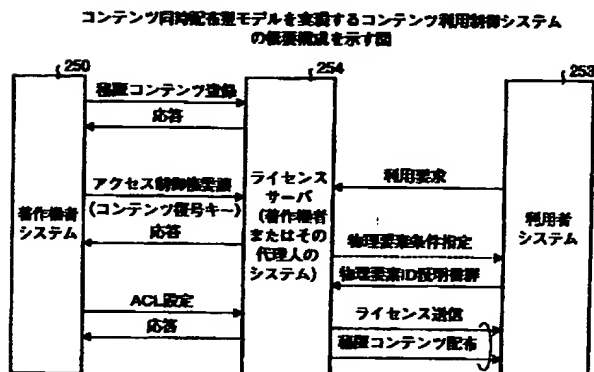
【図20】



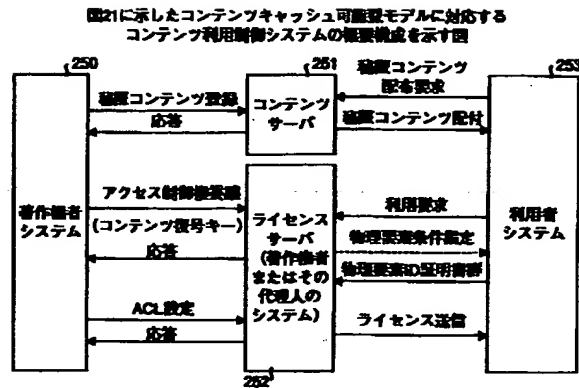
【図21】



【図23】



【図22】



フロントページの続き

(51)Int. Cl. ⁷	識別記号	F I	キーワード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D

(72)発明者 宮澤 雄司
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA03 AA06 BB09 BB10 CA16
5B085 AA08 AE08 AE23 AE29 BC02
BG02 BG07
5J104 AA12 AA16 EA04 EA15 MA01
NA02